Docket No. 45687-00036
P05139US00LH/maw

REMARKS

Favorable reconsideration of the above-identified application, as presently amended, is respectfully requested.

The amendments made to the claims herein are not being made in response to any prior art nor for any reason related to the statutory requirements for patentability. Applicant does not intend to narrow any claim element by the amendments made herein. No new matter has been added. Exhibit A, a marked-up copy of all claims amended herein, is attached to this Preliminary Amendment.

In view of the foregoing, Applicant respectfully requests the thorough reconsideration of this application and earnestly solicits an early notice of allowance.

Respectfully submitted,

JENKENS & GILCHRIST,
A Professional Corporation

Ross T. Robinson
Reg. No. 47,031

Dated: Sept. 25, 2002

1445 Ross Avenue, Suite 3200
Dallas, Texas 75202-2799
(214) 965-7300
(214) 855-4300 (fax)

EXHIBIT A
MARKED-UP CLAIM AMENDMENT(S)

1. (AMENDED) A method [method] for establishing security in an ad hoc communication network[(106)], the ad hoc communication network [(106)] comprising a set of communication nodes [(101, 103-105) whereof], at least two [of the] nodes of the set of communication nodes [(103-105)] having a mutual trust relation and [thus constituting]comprising a trust group [(102)], the trust relations being created with public keys, and at least one additional node [(101),] the at least one additional node being a candidate node for joining the trust group [(102)] within the ad hoc communication network, [(106), **characterised** by] the nodes having authority to delegate trust to nodes of the set of communication nodes they trust, the method comprising the steps of:

[-a)]identifying a node of the set of communication nodes [(103)] within the trust group having a trust relation with the candidate node[(101)], the node having the trust relation with the candidate node being an [a so-called] X-node [(103)]; and

[-b)]distributing trust relations between all [the] members in the trust group [(102)] and the candidate node [(101)] by means of the X-node [(103)].

2. (AMENDED) The method of claim 1, [**characterised** by] comprising, before the identifying step, the [further step of [to be taken before step a),] the candidate node [(101)] sending a message[,] comprising [its] a public key of the candidate node[,] to all nodes [(103-105)] of the set of communication nodes within the ad hoc communication network.

3. (AMENDED) The method of [any of the previous claims] claim 1, [**characterised** in that] wherein the ad hoc communication network [(106)] comprises a single trust group [(102),] and a single candidate node [(101)], and wherein the distributing step [b), implies that] comprises the X-node [(103) sends] sending a signed message[,] comprising a list of [the] nodes [(104, 105)] that the X-node [(103)] trusts within the ad hoc communication network [(106),] and [all their] all corresponding public keys to the candidate node [(101)].

4. (AMENDED) The method according to [any of the previous claims] claim 1, [**characterised** in that] wherein the distributing step [b) further implies that] comprises the X-node [(103) signs] signing the candidate node's [(101)] public key.

5. (AMENDED) The method according to [the previous] claim 4, [**characterised** in that] wherein the distributing step [b) further implies,] comprises the X-node [(103), sends] sending a message[,] comprising the candidate node's [(101)] signed public key[,] to the nodes [(104-105)] within the trust group [(102)].

6. (AMENDED) The method according to claim 2 [**characterised** in that], wherein the ad hoc communication network [(201)] comprises a set of nodes [(A-M)] comprising several trust groups, [(202-205), and all nodes (A-M)] each of the set of nodes being candidates for joining all trust groups[,] within the ad hoc communication network[,] that [they] the set of nodes are not already a member of, the method comprising [the further step to be taken, by each node (A-M)], after receiving the messages [from all candidate nodes (A-M)], each node of the set of nodes creating a list of [the] candidate nodes that [the particular node] a given node of the set of nodes trusts and [their] corresponding public keys.

7. (AMENDED) The method according to [the previous] claim 6, [**characterised** by] further comprising [the step of] deciding one node [(A)] within the ad hoc communication network [(201)] to act as a server node [(A)].

8. (AMENDED) The method according to [any of the claims 6-7] claim 7, [**characterised** by] further comprising [the step of,] the server node [(A)] receiving, from each other node [(B-M)] within the ad hoc communication network, a message comprising [its]a respective public key, [the]a respective list of [the] candidate nodes that the respective node [trust] trusts, and [their] corresponding public keys.

9. (AMENDED) The method according to [the previous] claim 8, [**characterised** by] further comprising [the step of,] the server node [(A)] classifying the at least one candidate node as being a server-trusted node [(B, C, D, E, F and I)] or as being a server-untrusted node [(G, H, J, K, L and M)], depending on whether the server node [(A)] trusts [it] the at least one candidate node or not.

10. (AMENDED) The method according to [the previous] claim 9, wherein [a server node trusting a server-untrusted node constitutes a so-called Y-node, **characterised** in that] the identifying step [a) implies that] further comprises [the step of] the server node [(A) identifies] identifying at least one Y-node required for distributing trust relations between the server node [(A)] and [as many] at least one server-untrusted node [nodes as possible].

11. (AMENDED) The method according to [the previous] claim 10, [**characterised** in] wherein said distributing step [b)] further comprises [implying that server node (A) sends] sending, by the server node, of a request to the identified at least one Y-node [Y-nodes (D, H) of distributing] to distribute said trust relations between the server node [A] and the server-untrusted nodes.

12. (AMENDED) The method according to [the previous] claim 11, [**characterised** in] wherein said distributing step [b)] further comprises [implying that server node (A) obtains] obtaining, by the server node, of said requested trust relations.

13. (AMENDED) The method according to [the previous] claim 12, [**characterised** in,] wherein the step of obtaining the trust relations further [comprising that] comprises:

[for each server-untrusted node that the Y- node have a trust relation with, the Y-node signs] signing, by the Y-node, of the public key of the server node for each server-untrusted node that the Y-node has a trust relation with; [(A)] and [forwards]

forwarding, by the Y-node, of said signed public key [it] to the server-untrusted node.

14. (AMENDED) The method according to [any of the claims 12-13] claim 12,[**characterised** in] wherein the step of obtaining the trust relations [comprising] comprises:

[that for each server-untrusted node that the Y-node have a trust relation with, the Y-node signs] signing, by the Y-node, of the public key of the server-untrusted node for each server-untrusted node that the Y-node has a trust relation with; and [forwards]

forwarding, by the Y-node, of said signed public key [it] to the server node [(A)].

15. (AMENDED) The method according to [any of the claims 12-14] claim 12, [**characterised** by] comprising the further step of[, server node (A)], after obtaining said trust relation, reclassifying, by the server node, the server-untrusted node with the obtained trust relation as being a server-trusted node.

16. (AMENDED) The method according to [any of the claims 12-15] claim 12, [**characterised** by] comprising the further step of[, server node (A)] sending, by the server node, of a signed message comprising the server node's [(A) all] trusted public keys belonging to trusted candidate nodes within the ad hoc communication network [(201)].

17. (AMENDED) An ad hoc communication network [(106)] comprising:

a set of communication nodes [(101, 103-105) whereof],

each node of said set of communication [the] nodes [(101, 103-105) each] comprising a receiver and a computer, the computer comprising a processor and a memory, each node [the nodes (101, 103-105)] being interconnected with communication links, at least two of the nodes [(103-105) are] having a mutual trust relation and [thus constituting]comprising a trust group [(102)], the trust relations being created with public keys, [and] at least one additional node of the set of communication nodes [(101)] being a candidate node for joining at least one trust group [(102)] within the ad hoc network, [**characterised** by]

the at least one candidate node [(101)] having means for requesting if any of the nodes

within the trust group [(102)] have a trust relation with the candidate node[(101)], and

each node [the nodes] being authorised to and [are] having means for[,] distributing trust relations between [its] the trust group [(102)] and the candidate node [(101)] that [it] the node trusts.

18. (AMENDED) The ad hoc communication network [(201)] according to [the previous] claim 17, [characterised by] wherein said each node [(A-M) having] comprises means for creating a list of [the] candidate nodes that [the] each node trusts and [their] corresponding public keys of each node[,] to be stored in the memory.

19. (AMENDED) The ad hoc communication network according to [any of the claims 17-18] claim 17, [characterised in that] wherein one node of the set of communication nodes [(A)] within the ad hoc network [(201) being] is operable as a server node [(A),] capable of administrate distribution of trust relations.

20. (AMENDED) The ad hoc communication network [(201)] according to [the previous] claim 19, [characterised by] wherein the server node [(A) having means for classifying] is operable to classify the at least one candidate node as being a server-trusted node [(B, C, D, E, F and I),] or as being a server-untrusted node [(G, H, J, K, L and M)], depending on whether the server node [(A)] trusts the at least one candidate node or not.

21. (AMENDED) The ad hoc communication network [(201)] according to [the previous] claim 20, wherein [a server-trusted node trusting a server-untrusted node constitutes a so-called Y-node characterised by] the server node [(A) having] comprises means for identifying at least one Y-node [(D, H)] required for distributing trust relations between the server node [A] and [the] server-untrusted nodes.

22. (AMENDED) The ad hoc communication network [(201)] according to [the previous] claim 21 [characterised by], wherein the server node [(A) having] comprises means for sending to each of said at least one Y-node [the identified Y-nodes (D, H),]:

a request as to which of the server-untrusted nodes [(G, H, J and M)] theY-node [(D, H)] has a trust relation with[,]; and

a request for distributing trust relations between the server node [(A)] and the requested server-untrusted nodes.

23. (AMENDED) The ad hoc communication network according to [any of the claims 20-22] claim 20, [characterised by] wherein the server node [(A) having] comprises means for distributing obtained trust relations to the nodes within the ad hoc communication network [(201)].